UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/536,033	03/27/2000	Mariusz H. Jakubowski	MS1-515US	4016

22801 7590 02/25/2005

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
TRAN, TONGOC	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 02/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/536,033	JAKUBOWSKI ET AL.	
	Examiner	Art Unit	
	Tongoc Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 October 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to Applicant's amendment filed on October 6, 2004. Claims 18, 23, 27 and 32-33 have been amended. Claims 1-36 are pending.

Response to Arguments

2. Applicant's arguments with respect to amended claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 8-9, 12-15 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke-Smith (U.S. Patent No. 5,548,648) in view of Colberg (U.S. Patent No. 6,6668,325).

In respect to claim 8, Yorke-Smith discloses a method comprising: segmenting a digital goods into a plurality of segments (see col. 3, lines 25-27); transforming data segments according to different protection techniques to produce a protected digital goods having a composite of variously protected segment (see col. 1, lines 58-67).

Yorke-Smith does not explicitly disclose but Colberg discloses selecting and transforming only the selected segments (see Abstract and col. 1, line 65-col. 2, line 9,

select subset of code). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the transformation of selected segment taught by Colberg with Yorke-Smith's teaching of segmenting and transforming digital goods in order to enhance software security based on desired level of obfuscation (see Colberg, Abstract).

In respect to claim 9, Yorke-Smith and Colberg disclose the method as recited in claim 8, wherein at least two of the segments overlap one another (see Colberg, e.g. Abstract and col. 1, line 65-col. 2, line 10 (subset of code), loop subroutine or loop iteration commonly found in programming code contains some identical data, i.e. Fig. 20c, for (i=1,i<n,i++)...for (i=1,i<n,i++))

In respect to claim 12, Yorke-Smith and Colberg disclose a method as recited in claim 8, wherein the transforming comprises:

Augmenting at least one segment using a certain protection technique (see col. 1, lines 48-65); and inserting a checkpoint, which may be used to evaluate a validity of the augmented segment, within the protected digital goods but outside of the augmented segment being evaluated (see Yorke-Smith, col. 3, lines 25-42).

In respect to claims 13 and 14, Yorke-Smith and Colberg disclose a method as recited in claim 8. Colberg further discloses comprising receiving quantitative parameters indicative of how much the protected digital goods should be altered and wherein the transforming is performed to satisfy the quantitative parameters (see Colberg, Abstract, col. 1, line 65-col. 2, line 10).

In respect to claim 15, Yorke-Smith and Colberg disclose a method as recited in claim 8. Colberg further discloses wherein the various forms of protection are selected from a group of protection tools comprising code integrity verification, acyclic code integrity verification, cyclic code integrity verification, secret key scattering, obfuscated function execution, encryption/decryption, probabilistic checking, Boolean check obfuscation, in-lining, reseeding pseudo random number generators with tune varying inputs, antidisassembly methods, varying execution paths between runs, anti-debugging methods, and time/space separation between tamper detection (see Colberg, Abstract and col. 1, line 65 to col. 2, line 10).

In respect to claim 17, the claim limitation is a computer-readable medium claim which is substantially similar to method claim 8 and therefore the same rejection applied.

4. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke-Smith (U.S. Patent No. 5,548,648) in view of Colberg (U.S. Patent No. 6,6668,325) in view of Simmon et al. (U.S. Patent No. 6,507,868, hereinafter Simmon).

In respect to claim 16, Yorke-Smith and Colberg disclose the method as recited in claim 8. Yorke-Smith and Colberg do not explicitly disclose wherein the applying comprises applying a form of protection in which a checksum can be computed on a set of bytes of the digital goods without actually reading the bytes. However, Simmon discloses performing checksum on data packet (Simmon, col. 16, lines 63-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made

to implement the encryption system of Yorke-Smith, Sung and Colberg with testing the checksum taught by Simmon to ensure transmitted data has not been tampered during the transmission.

5. Claims 18 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke-Smith (U.S. Patent No. 5,548,648) in view of Gutowitz (U.S. Patent No. 5,365,589)

In respect to claim 18, Yorke-Smith discloses a method comprising:

parsing the software product into code sections segments (see Yorke-Smith, col. 3, lines 25-27);

selecting at least one code section (see col. 1, lines 53-55); augmenting the selected code section to add protection qualities (see col. 1, lines 58-67); repeating the selecting and the augmenting for different code sections until the desired quantity of protection has been applied (see col. 1, lines 48-67).

Yorke-Smith does not explicitly disclose establishing parameters prescribing a desired quantity of protection to be applied to a software product and augmenting the selected code section to add protection qualities (partially encrypting code section). However, Gutowitz discloses partially encrypting image file (see col. 35, lines 39-67). It would have been obvious to one of ordinary skill in the art to combine the teaching of Yorke-Smith's encryption method for encrypting data into a plurality of controlled and

data blocks with Gutowitz's teaching of partially encrypting digital data so that it enables information of different levels of security and/or destined for different uses to encrypted into the same ciphertext (see Gutowitz, col. 35, lines 64-66).

In respect to claim 22, the claim limitation is a computer-readable medium claim which is substantially similar to method claim 18 and therefore the same rejection applied.

6. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke-Smith (U.S. Patent No. 5,548,648) and Gutowitz (U.S. Patent No. 5,365,589) and further in view of Levit (U.S. Patent No. 5,420,942).

In respect to claim 19, Yorke-Smith and Gutowitz disclose a method as recited in claim 18. York-Smith does not explicitly disclose wherein the establishing comprises enabling a user to enter the parameters. However, Levit discloses allowing user manually entering parameter (see Levit, col. 8, line 67--col. 9, line 3). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Yorke-Smith's encryption system that allow the user to enter the parameters for the benefit of having user to decide what program data to be encrypted instead of the software to do the task.

7. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke-Smith (U.S. Patent No. 5,548,648) and Gutowitz (U.S. Patent No. 5,365,589) and further in view of Colberg (U.S. Patent No. 6,668,325).

In respect to claim 20, Yorke-Smith and Gutowitz disclose a method as recited in claim 18. Yorke-Smith and Gutowitz do not explicitly disclose wherein the augmenting comprises applying a protection technique selected from a group of protection techniques comprising code integrity verification, acyclic code integrity verification, cyclic code integrity verification, secret key scattering, obfuscated function execution, encryption/decryption, probabilistic checking, Boolean check obfuscation, in-lining, reseeding pseudo random number generators with tune varying inputs, anti-disassembly methods, varying execution paths between runs, anti-debugging methods, and timespace separation between tamper detection and response (see Colberg, Abstract and col. 1, line 65-col. 2, line 10). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the encryption system taught by Yorke-Smith and Gutowitz with these specific protective tools because the more protective tools is used the harder it is for the data to be tampered with.

8. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke-Smith (U.S. Patent No. 5,548,648) in view of Gutowitz (U.S. Patent No. 5,365,589) and further in view of Simmon et al. (U.S. Patent No. 6,507,868, hereinafter Simmon).

In respect to claim 21, Yorke-Smith and Gutowitz do not disclose a method as recited in claim 18, wherein the augmenting comprises applying a protection technique in which a checksum can be computed on a set of bytes of the digital goods without actually reading the bytes. However, Simmon discloses performing checksum on data

packet (Simmon, col. 16, lines 63-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Yorke-Smith and Gutowitz's encryption system with Simmon's teaching using checksum to test data packet to ensure transmitted data has not been tampered during the transmission.

9. Claims 1-5, 7, 10-11, 23-24 and 26-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke-Smith (U.S. Patent No. 5,548,648) in view of Sung (U.S. Patent No. 5,768,372) and further in view of Colberg et al. (U.S. Patent No. 6,668,325)

In respect to claim 1, Yorke-Smith discloses a method comprising:

receiving an original digital good; and applying various forms of protection to the original digital goods to produce a protected digital goods (see Yorke-Smith Abstract and col. 1, lines 48-67, col. 2, lines 50-65).

Yorke-Smith does not explicitly disclose applying randomly various forms of protection. However, Sung discloses randomly selects which of the encryption to use (see Sung Abstract and col. 6, lines 32-40). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Yorke-Smith for applying various forms of protection with Sung's teaching of selecting encryption randomly for a more secure data protection, because a person attempting to copy the programming data would not be able to know which encryption is being used even if all the potential encryptions is known (see Sung, col. 3, lines 14-20).

Furthermore, Yorke-Smith does not disclose but Colberg discloses at least two of the segments overlap one another wherein overlapping segments are different from

each other but include some identical data (see Colberg, e.g. Abstract and col. 1, line 65-col. 2, line 10 (subset of code), loop subroutine or loop iteration commonly found in programming code contains some identical data, i.e. Fig. 20c, for (i=1,i<n,i++)...for (i=1,i<n,i++)) . Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Yorke-Smith's segmenting data with various encryption protection with Colberg's segments overlap another and other to enhance software security.

In respect to claim 2, Yorke-Smith, Sung and Colberg disclose a method as recited in claim 1, wherein the randomly applying comprises pseudo randomly applying the various forms of protection according to pseudo random techniques (see Sung, col. 4, lines 20-30).

In respect to claim 3, Yorke-Smith, Sung and Colberg disclose a method as recited in claim 1, wherein the applying comprises randomly selecting the forms of protection from a set of available forms of protection (see Sung, col. 6, lines 32-40).

In respect to claim 4, Yorke-Smith, Sung and Colberg disclose a method as recited in claim 1, wherein the applying comprises applying the various forms of protection to randomly selected portions of the original digital goods (see Sung, 3, lines 14-20).

In respect to claim 5, Yorke-Smith, Sung and Colberg disclose a method as recited in claim 1. Colberg further disclose wherein the various forms of protection are selected from a group of protection tools comprising code integrity verification, acyclic code integrity verification, cyclic code integrity verification, secret key scattering,

obfuscated function execution, encryption/decryption, probabilistic checking, Boolean check obfuscation, in-lining, reseeding pseudo random number generators with tune varying inputs, anti-disassembly methods, varying execution paths between runs, anti-debugging methods, and timespace separation between tamper detection and response (see Colberg, Abstract and col. 1, line 65-col. 2, line 10).

In respect to claim 7, the claim limitation is a computer-readable medium claim which is substantially similar to method claim 1 and therefore the same rejection applied.

In respect to claim 10, York-Smith and Colberg do not disclose but Sung discloses explicitly disclose a method as recited in claim 8, wherein the selecting comprises randomly selecting the segments (see col. 3, lines 1-20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Yorke-Smith's encryption method for encrypting data into a plurality of controlled and data blocks with Sung's teaching of randomly selecting the segments for a more secure data transmission because even if all the potential encryptions is known, one has to know which encryption is associated with a particular encryption selection data (see Sung, col. 3, lines 16-20).

In respect to claim 11, York-Smith and Colberg do not explicitly disclose but Sung discloses a method as recited in claim 8, wherein the transforming comprises transforming the selected segments according to randomly chosen protection techniques (see Sung, col. 1-20). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of

Yorke-Smith's encryption method for encrypting data into a plurality of controlled and data blocks with Sung's teaching of selecting encryption randomly for a more secure data protection because in order for a person to know which encryption from among all the available encryptions is associated with a particular encryption selection data (see Sung, col. 3, lines 15-20).

In respect to claim 23, York-Smith discloses a production system, comprising: a memory to store an original digital goods (see col. 1, 1-10 and lines 48-52); and a production server equipped with a set of multiple protection tools that may be used to augment the original digital goods for protection purposes (see col. 1, lines 4-10 and col. 48-52), the production server being configured to parse the original digital goods (see cot. 1, lines 48-67, col. 3, lines 25-27).

Yorke-Smith does not disclose but Sung discloses apply protection tools selected from the set of protection tools to the original digital goods in a random manner to produce a protected digital goods (see Sung, col. 3, lines 1-20). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Yorke-Smith's encryption method for encrypting data into a plurality of controlled and data blocks with Sung's teaching of selecting encryption randomly for a more secure data protection because in order for a person to know which encryption from among all the available encryptions is associated with a particular encryption selection data (Sung, col. 3, lines 15-20).

Furthermore, Yorke-Smith does not explicitly disclose but Colberg discloses transforming only the selected portions of the original digital good (see Abstract and col.

1, line 65-col. 2, line 9, select subset of code). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the transformation of selected segment taught by Colberg with Yorke-Smith's teaching of segmenting and transforming digital goods in order to enhance software security based on desired level of obfuscation (see Colberg, Abstract).

In respect to claim 26, Yorke-Smith, Sung and Colberg disclose a production system as recited in claim 23, wherein the production server has a pseudo random generator to introduce randomness into the application of the protection tools to various portions of the original digital goods (see Sung, col. 4, lines 20-30).

In respect to claims 24, 28 and 36, the claim limitation are substantially similar to claim 5. Therefore, claims 24 and 36 are rejected based on the similar rationale.

In respect to claim 27, the claim limitation is substantially similar to claim 23. Therefore, claim 27 is rejected based on the similar rationale.

In respect to claim 29, the claim limitation is substantially similar to claim 2. Therefore, claim 29 is rejected based on the similar rationale.

In respect to claim 30, the claim limitation is substantially similar to claim 26. Therefore, claim 30 is rejected based on the similar rationale.

In respect to claim 31, Yorke-Smith, Sung and Colberg disclose an obfuscation system as recited in claim 27, further comprising: a quantitative unit to specify a quantity of protection qualities to be added to the digital good (Colberg, Abstract and col. 1, line 65-col. 2, line 10).

In respect to claim 32, Yorke-Smith discloses a client-server system, comprising: a production server to apply various forms of protection to a digital goods to produce a protected digital goods (see col. 1, lines 48-67); and a client to store and execute the protected digital goods the client being configured to evaluate the protected digital good (see Yorke-Smith, col. 1, lines 1-10, 48-67, col. 3, lines 5-12 and col. 5, lines 23-25).

Yorke-Smith does not disclose but Sung discloses randomly applying various forms of protection to a digital goods (see Sung, col. 6, lines 31-40). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Yorke-Smith's encryption method for encrypting data into a plurality of controlled and data blocks with Sung's teaching of selecting encryption randomly for a more secure data protection because a person attempting to copy the programming data would not be able to know which encryption is being used even if all the potential encryptions is known (see Sung, col. 3, lines 14-20).

Yorke-Smith does not explicitly disclose but Colberg discloses transforming only the selected portions of the original digital good (see Abstract and col. 1, line 65-col. 2, line 9, select subset of code). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the transformation of selected segment taught by Colberg with Yorke-Smith's teaching of segmenting and transforming digital goods in order to enhance software security based on desired level of obfuscation (see Colberg, Abstract).

In respect to claim 33, the claim limitation is a computer-readable media claim which is substantially similar to method claim 23 and therefore the same rejection applied.

In respect to claim 34, Yorke-Smith, Sung and Colberg disclose one or more computer-readable media as recited in claim 33. Sung further discloses comprising computer-executable instructions to randomly select the protection, tools from a set of available protection tools (see Sung, col. 6, lines 32-40).

In respect to claim 35, Yorke-Smith, Sung and Colberg disclose one or more computer-readable media as recited in claim 33. Sung further discloses comprising computer-executable instructions to apply the protection tools to randomly selected portions of the original digital goods (see Sung, col. 3, lines 1-20 and col. 6, lines 32-40).

10. Claims 6 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke-Smith (U.S. Patent No. 5,548,648) in view of Sung et al. (U.S. Patent No. 5,768,372) and Colberg (U.S. Patent No. 6,668,325) and further in view of Simmon et al. (U.S. Patent No. 6,507,868).

In respect to claim 6, Yorke-Smith, Sung and Colberg disclose method as recited in claim 1. Yorke-Smith, Sung and Colberg do not explicitly disclose wherein the applying comprises applying a form of protection in which a checksum can be computed on a set of bytes of the digital goods without actually reading the bytes. However, Simmon discloses performing checksum on data packet (Simmon, col. 16, lines 63-67).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the encryption system of Yorke-Smith, Sung and Colberg with testing the checksum taught by Simmon to ensure transmitted data has not been tampered during the transmission.

In respect to claim 25, the claim limitation is substantially similar to claim 6. Therefore, claim 25 is rejected based on the similar rationale.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran
Art Unit: 2134

TT

February 16, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100